Fifty-first Annual Allerton Conference
Allerton House, UIUC, Illinois, USA
October 2 - 3, 2013

How Many Antennas Does a Cooperative Jammer Need for Achieving the Degrees of Freedom of Multiple Antenna Gaussian Channels in the Presence of an Eavesdropper?

Mohamed Nafea Aylin Yener

Wireless Communications and Networking Laboratory (WCAN)
Electrical Engineering Department
The Pennsylvania State University, University Park, PA 16802.
msn139@psu.edu *yener@engr.psu.edu*

***Abstract*—In this work, multiple antenna Gaussian wiretap channels with a multiantenna cooperative jammer are considered. In particular, the focus is on identifying the spatial resources needed at the cooperative jammer in order to achieve a secure degrees of freedom (s.d.o.f.) for the channel in question equal to the degrees of freedom (d.o.f.). In order to accomplish this goal, the cooperative jammer sets out to send correlated jamming signals. Simultaneously, the legitimate transmitter chooses a precoder that perfectly aligns its information signals over the jamming ones at the eavesdropper. Both terminals use structured signaling, i.e., discrete constellations. The proposed approach is shown to achieve full d.o.f. for the channel at hand as long as the cooperative jammer has twice the antennas of the eavesdropper. It is also shown that within $\frac{1}{2}$ of the d.o.f. is achievable with one less antenna at the cooperative jammer.**

I. Introduction

Information theoretic framework for confidentiality of transmitted messages was established in [1]. In this work, Shannon considered noiseless channels from the transmitter to the legitimate receiver and the eavesdropper and showed that achieving perfect secrecy requires encrypting the message with a key that has a rate equal to the message rate. Wyner in [2] introduced the wiretap channel and showed that, for noisy channels, a non-zero secrecy capacity can be achieved as long as the channel from the transmitter to the eavesdropper is degraded with respect to the one to the legitimate receiver. This result was later extended to more general discrete memoryless channels in [3]. Secrecy capacity of the scalar Gaussian wiretap channel was obtained in [4].

Multi-terminal models of the wiretap channel were extensively studied, see for example [5]–[13]. As evidenced by these previous studies, it is challenging to find the exact secrecy capacity in most scenarios. Instead, for Gaussian channels, the high signal to noise ratio (SNR) behavior of the secrecy capacity, i.e., the secure degrees of freedom (s.d.o.f.), has been investigated by many [14]–[18]. In these studies, not surprisingly, it is observed that the imposition of the secrecy constraint decreases the achievable d.o.f.

A model of particular interest is the Gaussian wiretap channel where it is known that the secrecy capacity does not scale with the SNR resulting in zero s.d.o.f., even when an external terminal, i.e., a cooperative jammer [9], sets out to reduce the reception quality of the eavesdropper [19]. A remedy for this shortcoming is to employ structured signaling both by the cooperative jammer and the legitimate transmitter [15], [20]. The scaling of the secrecy rate with power results due to unfavorable alignment of structured signals from the legitimate transmitter and the cooperative jammer at the eavesdropper while causing little harm at the legitimate receiver [20]. In recent work, reference [17] has shown that by employing multiple cooperative jammers and structured signaling, it is possible to approach s.d.o.f. of 1 for the Gaussian wiretap channel.

In addition to these developments for single antenna channels, multiple antennas have also been used extensively for improving the secrecy rates of various channel models [21]–[26]. Recent reference [22] uses a multiple antenna cooperative jammer to maintain the s.d.o.f. at $\frac{1}{2}$ when the eavesdropper has multiple antennas while the legitimate terminals have one antenna each.

In this paper, we consider multiple antenna Gaussian wiretap channels with an external terminal to help with confidential communication between legitimate terminals in the presence of an eavesdropper, i.e., a cooperative jammer that also has multiple antennas. Specifically, we investigate the conditions under which the cooperative jammer can help the system achieve its full degrees of freedom (d.o.f.) as if the eavesdropper does not exist. That is, we are interested in identifying the number of antennas needed at the cooperative jammer in order to get rid of the secrecy penalty on the degrees of freedom.

Recognizing that in order to purge the cost of secrecy on the d.o.f. altogether, the cooperative jammer needs to send jamming signals that cause no interference at the legitimate receiver and completely cover the secret message at the eaves-

978-1-4799-3410-2/13/$31.00 ©2013 IEEE

dropper at the same time, we consider that the cooperative jammer transmits coordinated signals over the directions that are invisible to the legitimate receiver, i.e., over the null space of the channel from the cooperative jammer to the legitimate receiver. Simultaneously, the transmitter precodes its transmitted signals so that they align perfectly with the jamming signals at the eavesdropper. We note that Gaussian or structured signaling can be used with the achievable scheme, and choose to use structured signaling for its simplicity of implementation and analysis.

For a Gaussian wiretap channel with N antennas at the transmitter, legitimate receiver, and the eavesdropper, we first consider the approach in which the cooperative jammer transmits its jamming signals over the null space of its channel to the legitimate receiver. Next, we consider a special case of the null space approach which amounts to the cooperative jammer transmitting signals designed to cancel each other at the legitimate receiver. In both approaches, we show that it is possible to achieve N s.d.o.f. for this channel with the help of a cooperative jammer that has $2N$ antennas.

Finally, we investigate the achievable s.d.o.f with removing one antenna from the cooperative jammer. We show that s.d.o.f. of $N - \frac{1}{2}$ is achievable when the cooperative jammer has $2N-1$ antennas. In this scheme, we need that at least one information and one jamming signal to have a discrete constellation, i.e., structured signaling.

The remainder of the paper is organized as follows. Section II introduces the model and the definitions. The null space approach is considered in Section III. In section IV, jamming cancellation is considered. Section V investigates the achievable s.d.o.f. with one less antenna at the cooperative jammer. Section VI concludes the paper.

Notation: We denote the set of integers $\{-Q, -Q+1, \cdots, Q-1, Q\}$ by $(-Q, Q)_{\mathbb{Z}}$. We use lower case font to denote scalars and upper case font to denote random variables. We denote random vectors and matrices with bold upper case letters, where the distinction is clear from the context. $\mathbf{I}_N$ is a $(N \times N)$ identity matrix and $\mathbf{0}_N$ is a $(N \times N)$ matrix of zeros. The null space of a matrix $\mathbf{A}$ is denoted by $\mathcal{N}(\mathbf{A})$.

II. Channel Model and Definitions

We consider a Gaussian wiretap channel composed of one transmitter, one receiver, an external eavesdropper, and an external cooperative jammer as shown in Fig. 1. The transmitter, legitimate receiver, and the eavesdropper are all equipped with N antennas each. The cooperative jammer is equipped with M antennas.

The signal vectors received at the legitimate receiver and the eavesdropper in one channel use can be expressed as

$$\mathbf{Y}_r = \mathbf{H}_t\mathbf{X}_t + \mathbf{H}_c\mathbf{X}_c + \mathbf{Z}_r \qquad (1)$$

$$\mathbf{Y}_e = \mathbf{G}_t\mathbf{X}_t + \mathbf{G}_c\mathbf{X}_c + \mathbf{Z}_e, \qquad (2)$$

where $\mathbf{X}_t = [X_{t_1} X_{t_2} \cdots X_{t_N}]^T$, $\mathbf{X}_c = [X_{c_1} X_{c_2} \cdots X_{c_M}]^T$ are the transmitted signal vectors from the transmitter and the cooperative jammer. $\mathbf{H}_t, \mathbf{G}_t \in \mathbb{R}^{N\times N}$are the channel gain matrices from the transmitter to the legitimate receiver and to the eavesdropper, respectively. $\mathbf{H}_c, \mathbf{G}_c \in \mathbb{R}^{N\times M}$ are the channel gain matrices from the cooperative jammer to the legitimate receiver and to the eavesdropper.

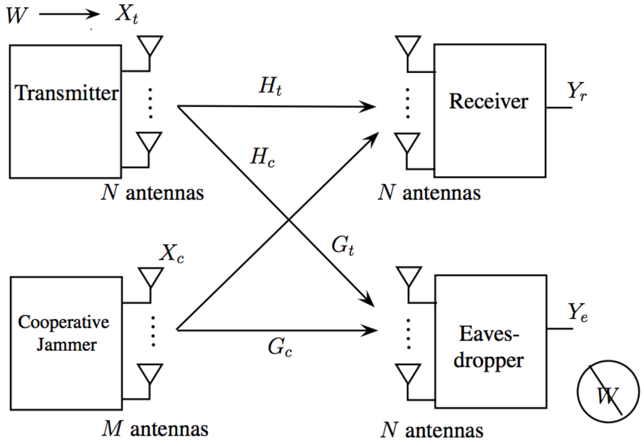

Fig. 1: Gaussian wiretap channel with N antennas at the transmitter, receiver, and the eavesdropper, and M antennas at the cooperative jammer.

The channel gains are assumed to be constant, independently drawn from a real-valued[1] continuous distribution, and known at all terminals. $\mathbf{Z}_r$ and $\mathbf{Z}_e$ are the additive Gaussian noise vectors at the legitimate receiver and the eavesdropper, respectively. The entries of $\mathbf{Z}_r$ and $\mathbf{Z}_e$ are assumed to be independent and identically distributed (i.i.d.) zero mean unit variance Gaussian random variables. The power constraints on the transmitter and the cooperative jammer are $E\left[\mathbf{X}_t^T\mathbf{X}_t\right] \leq P$ and $E\left[\mathbf{X}_c^T\mathbf{X}_c\right] \leq P$.

The transmitter aims to communicate with the legitimate receiver while keeping the transmitted message secret from the external eavesdropper. The transmitter employs a stochastic encoder. Secrecy rate R_s is achievable if there exists a channel code such that (i) the probability of decoding error at the legitimate receiver and (ii) the mutual information per channel use between the secret message and the eavesdropper's received signal both vanish[2]. The achievable secure degrees of freedom (s.d.o.f.) is defined as $D_s = \lim_{P\to\infty} \frac{R_s}{\frac{1}{2}\log P}$.

The cooperative jammer transmits in order to assist the legitimate transmitter-receiver pair in achieving the full d.o.f. of the channel with secrecy.

III. Null Space Approach

As long as it has the sufficient number of antennas, we can have the cooperative jammer transmit the jamming signals over the null space of its channel gain matrix to the legitimate receiver, $\mathbf{H}_c$, so that, the jamming signals do not interfere with the legitimate receiver at all. Consider the system model depicted in Fig. 1. The received signal vectors at the legitimate

[1] The assumption of real-valued channel gains can be removed when Gaussian signaling is considered.

[2] We consider weak secrecy throughout the paper.

receiver and the eavesdropper are expressed as in (1) and (2), respectively.

In order to achieve full d.o.f. in the presence of the secrecy constraint, the transmitter needs to transmit N independent information streams reliably. These N information streams are precoded into the N transmitted signals at the transmitter in each channel use. On the other hand, in order to perfectly cover these N information streams at the eavesdropper, N independent jamming streams are needed at the cooperative jammer. These jamming streams at the cooperative jammer are also precoded into the transmitted jamming signals. The transmitted jamming signals have to be invisible at the legitimate receiver in order to recover the full d.o.f. N.

Providing non-zero vectors in the null space of $\mathbf{H}_c$ requires the number of antennas at the cooperative jammer to be greater than N. In addition, each of the N independent jamming streams has to be transmitted over an independent direction so that the precoding matrix at the transmitter, that is chosen to align the N information streams over the jamming ones at the eavesdropper, is full rank. Therefore, the null space of $\mathbf{H}_c$ has to be of dimension N, and hence, $M = 2N$ antennas at are sufficient for the cooperative jammer with this approach.

The encoding scheme consists of two parts. The jamming streams are transmitted over the null space of $\mathbf{H}_c$. The transmitter chooses a precoder $\mathbf{P}_t$ that aligns its N information streams over the jamming signals at the eavesdropper. The transmitted signal vectors from the transmitter and the cooperative jammer are given by

$$\mathbf{X}_t = \mathbf{P}_t \mathbf{U}_t \tag{3}$$

$$\mathbf{X}_c = \mathbf{J}_c \mathbf{V}_c, \tag{4}$$

where[3] $\mathbf{U}_t = [U_1 \; U_2 \; \cdots \; U_N]^T$ and $\mathbf{V}_c = [V_1 \; V_2 \; \cdots \; V_N]^T$. U_i and V_i, $i = 1, 2, \ldots, N$, are the N i.i.d. information streams and the N i.i.d. jamming streams, respectively. Each of U_i and V_i, for all $i = 1, 2, \cdots, N$, is uniformly distributed over the set $(-Q, Q)_{\mathbb{Z}}$, where Q is an integer whose value is in accordance with the power constraints on the transmitted signals from the transmitter and the cooperative jammer. $\mathbf{J}_c \in \mathbb{R}^{2N \times N}$ is a matrix whose N columns are chosen to span $\mathcal{N}(\mathbf{H}_c)$.

Substituting (3) and (4) in (1) and (2), the received signal vectors at the legitimate receiver and the eavesdropper are

$$\mathbf{Y}_r = \mathbf{H}_t \mathbf{P}_t \mathbf{U}_t + \mathbf{Z}_r \tag{5}$$

$$\mathbf{Y}_e = \mathbf{G}_t \mathbf{P}_t \mathbf{U}_t + \mathbf{G}_c \mathbf{J}_c \mathbf{V}_c + \mathbf{Z}_e. \tag{6}$$

The N rows of $\mathbf{G}_c$ are almost surely linearly independent since all of its entries are drawn from a continuous distribution. Moreover, the N columns of $\mathbf{J}_c$ are N linearly independent vectors chosen from the null space of $\mathbf{H}_c$. The multiplication of $\mathbf{G}_c$ and $\mathbf{J}_c$ can be viewed as N linear combinations of the $2N$ length-N rows of $\mathbf{J}_c$ with the independently generated coefficients that are the entries on the rows of $\mathbf{G}_c$. This results in $\mathbf{G}_c\mathbf{J}_c$ is almost surely a full rank matrix. The proof is given in the Appendix.

In order to perfectly align the information streams over the jamming ones at the eavesdropper, the transmitter chooses the precoder $\mathbf{P}_t$ such that

$$\mathbf{P}_t = \mathbf{G}_t^{-1} \mathbf{G}_c \mathbf{J}_c. \tag{7}$$

Note that it is necessary for the precoder $\mathbf{P}_t$ to be a full rank matrix so that the N information streams are decoded at the legitimate receiver.

Substituting (7) in (6), the received signal vector at the eavesdropper is given by

$$\mathbf{Y}_e = \mathbf{G}_c \mathbf{J}_c (\mathbf{U}_t + \mathbf{V}_c) + \mathbf{Z}_e. \tag{8}$$

Since $\mathbf{X}_t$ and $\mathbf{X}_c$ are independent and the channel is memoryless, the secrecy rate

$$R_s = I(\mathbf{X}_t; \mathbf{Y}_r) - I(\mathbf{X}_t; \mathbf{Y}_e) \tag{9}$$

is achievable [3]. We lower bound this achievable secrecy rate as follows.

First, in order to compute $I(\mathbf{X}_t; \mathbf{Y}_r)$, it is sufficient to note that the signal observed by the legitimate receiver $\mathbf{Y}_r$ in (5) is a noisy version of the transmitted signal $\mathbf{X}_t$, i.e., the channel between the transmitter and the legitimate receiver is equivalent to a point-to-point N-antenna additive white Gaussian noise (AWGN) channel. Thus, the term $I(\mathbf{X}_t; \mathbf{Y}_r)$ can be expressed as

$$I(\mathbf{X}_t; \mathbf{Y}_r) = \frac{N}{2} \log P + o(\log P), \tag{10}$$

where $o(.)$ is

$$\lim_{P \to \infty} \frac{o(\log P)}{\log P} = 0. \tag{11}$$

Next, using (3) and (8), the term $I(\mathbf{X}_t; \mathbf{Y}_e)$ can be upper bounded as follows:

$$\begin{aligned}
I(\mathbf{X}_t; \mathbf{Y}_e) &\leq I(\mathbf{X}_t; \mathbf{Y}_e \mathbf{Z}_e) && (12)\\
&= I(\mathbf{X}_t; \mathbf{Y}_e | \mathbf{Z}_e) && (13)\\
&= I(\mathbf{X}_t; \mathbf{Y}_e - \mathbf{Z}_e) && (14)\\
&= H(\mathbf{Y}_e - \mathbf{Z}_e) - H(\mathbf{Y}_e - \mathbf{Z}_e | \mathbf{X}_t) && (15)\\
&= H(U_1 + V_1, U_2 + V_2, \cdots, U_N + V_N) \\
&\qquad - H(V_1, V_2, \cdots, V_N) && (16)\\
&\leq \log(4Q+1)^N - \log(2Q+1)^N && (17)\\
&= N \log \frac{(4Q+1)}{(2Q+1)} && (18)\\
&\leq N. && (19)
\end{aligned}$$

where (13) follows since $\mathbf{X}_t$ and $\mathbf{Z}_e$ are independent, and the inequality in (17) follows since the entropy of a uniform random variable over the set $(-2Q, 2Q)_{\mathbb{Z}}$ is an upper bound for the entropy of $U_i + V_i$, for all $i = 1, 2, \cdots, N$.

Thus, using (10) and (19), the achievable secrecy rate for the channel in interest can be expressed as

$$R_s = I(\mathbf{X}_t; \mathbf{Y}_r) - I(\mathbf{X}_t; \mathbf{Y}_e) \tag{20}$$

$$\geq \frac{N}{2} \log P + o(P) - N. \tag{21}$$

[3] Throughout this paper, we call $\mathbf{U}_t$ the information streams and $\mathbf{V}_c$ the jamming streams.

Hence, the achievable secure degrees of freedom is

$$D_s = \lim_{P\to\infty} \frac{R_s}{\frac{1}{2}\log P} \tag{22}$$

$$\geq \lim_{P\to\infty} \frac{\frac{N}{2}\log P + o(P) - N}{\frac{1}{2}\log P} \tag{23}$$

$$= N. \tag{24}$$

Since, with no secrecy constraint, the d.o.f. of the N-antenna Gaussian channel is N, the upper bound on the s.d.o.f. of a Gaussian wiretap channel with N antennas at each of the transmitter, legitimate receiver and the eavesdropper, naturally follows as N. Thus, with the use of $2N$-antenna cooperative jammer, the s.d.o.f. of this Gaussian wiretap channel is N.

IV. Jamming Cancellation

In this section, we consider jamming cancellation at the legitimate receiver which is a special case of the null space approach in the previous section. In this case, the cooperative jammer transmits coordinated jamming signals which are designed to cancel each other at the legitimate receiver. For clarity of exposition, we first consider the case $N = 1$ and $M = 2$, i.e., the transmitter, legitimate receiver and the eavesdropper are equipped with one antenna each and the cooperative jammer has two antennas. Next, we extend the approach to $N > 1$ in Section IV-B.

A. Single Antenna Gaussian Wiretap Channel

The signals observed at the legitimate receiver and the eavesdropper in (1) and (2) reduce to

$$Y_r = h_t X_t + h_{c_1} X_{c_1} + h_{c_2} X_{c_2} + Z_r \tag{25}$$

$$Y_e = g_t X_t + g_{c_1} X_{c_1} + g_{c_2} X_{c_2} + Z_e, \tag{26}$$

where h_{c_i} and g_{c_i} are the channel gains from the ith antenna of the cooperative jammer to the legitimate receiver and the eavesdropper, respectively, and $i = 1, 2$. X_{c_i} is the transmitted signal from the ith antenna of the cooperative jammer.

The transmitted signals from the legitimate transmitter and the cooperative jammer are expressed as

$$X_t = \alpha U \tag{27}$$

$$\mathbf{X}_c = \begin{bmatrix} \frac{1}{h_{c_1}} & \frac{-1}{h_{c_2}} \end{bmatrix}^T V. \tag{28}$$

where U and V are i.i.d. uniform over the set $(-Q, Q)_{\mathbb{Z}}$. The jamming stream V is transmitted from the cooperative jammer. The precoder α is used to align U over V at the eavesdropper.

From (28), it is easy to see that the two transmitted jamming signals are scaled so that they arrive at the legitimate receiver out of phase, and cancel each other completely. Since the channel gains are randomly drawn from a continuous distribution, the probability that the two jamming signals cancel each other at the eavesdropper is zero. The value of the precoder α is chosen such that the information stream U arrives at the eavesdropper with the same scaling as that for the jamming stream V.

The received signals at the legitimate receiver and the eavesdropper can be expressed as

$$Y_r = \alpha h_t U + Z_r \tag{29}$$

$$Y_e = \alpha g_t U + \beta V + Z_e, \tag{30}$$

where,

$$\beta = \left(\frac{g_{c_1}}{h_{c_1}} - \frac{g_{c_2}}{h_{c_2}} \right). \tag{31}$$

Let us choose the value of α such that $\alpha = \frac{1}{g_t}\beta$. We have

$$Y_r = \beta \frac{h_t}{g_t} U + Z_r \tag{32}$$

$$Y_e = \beta(U + V) + Z_e. \tag{33}$$

Using a similar analysis as in the previous section, it can be shown that the achievable s.d.o.f. of this channel is 1.

It is worth noting that if two separate single antenna cooperative jammers are used instead of the two-antenna cooperative jammer, the s.d.o.f. is $\frac{2}{3}$ [17]. The enabler of achieving 1 s.d.o.f. is the coordination between the two jamming signals at the two antennas of the cooperative jammer.

B. Multiple-antenna Gaussian Wiretap Channel

In this subsection, we extend the jamming cancellation technique to the case of an arbitrary N, i.e., the number of antennas at each of the transmitter, the legitimate receiver, and the eavesdropper. The observed signal vectors at the legitimate receiver and the eavesdropper are expressed as in (1) and (2), respectively, with $M = 2N$.

Similar to the previous section, the encoding scheme consists of two separate parts. First, the cooperative jammer precodes its N independent jamming streams into $2N$ jamming signals that cancel each other at the legitimate receiver. Next, the transmitter chooses a precodig matrix that aligns the information streams over the jamming ones at the external eavesdropper.

The singular value decomposition of $\mathbf{H}_c$ is

$$\mathbf{H}_c = \mathbf{Q}_c \mathbf{\Lambda}_c \mathbf{S}_c^T, \tag{34}$$

where $\mathbf{Q}_c \in \mathbb{R}^{N\times N}$ and $\mathbf{S}_c \in \mathbb{R}^{2N\times 2N}$ are unitary matrices. The matrix $\mathbf{\Lambda}_c \in \mathbb{R}^{N\times 2N}$ is given by

$$\mathbf{\Lambda}_c = \left[\mathbf{\Omega}_c \;\; \mathbf{0}_N\right], \tag{35}$$

where $\mathbf{\Omega}_c$ is a diagonal matrix composed of singular values of $\mathbf{H}_c$, i.e., $\mathbf{\Omega}_c = \text{diag}\left(\sigma_c^{(1)}, \sigma_c^{(2)}, \cdots, \sigma_c^{(N)}\right)$.

Let us write $\mathbf{S}_c^T$ as

$$\mathbf{S}_c^T = \mathbf{F}\overline{\mathbf{S}}_c, \tag{36}$$

where $\mathbf{F} \in \mathbb{R}^{2N\times 2N}$ is a full rank matrix which is given by

$$\mathbf{F} = \begin{bmatrix} \mathbf{I}_N & \mathbf{I}_N \\ \mathbf{0}_N & \mathbf{I}_N \end{bmatrix}. \tag{37}$$

Notice that $\overline{\mathbf{S}}_c$ is also a full rank matrix which is given by $\overline{\mathbf{S}}_c = \mathbf{F}^{-1}\mathbf{S}_c^T$. We can rewrite (34) as

$$\mathbf{H}_c = \mathbf{Q}_c \left[\boldsymbol{\Omega}_c \ \ \mathbf{0}_N\right] \begin{bmatrix} \mathbf{I}_N & \mathbf{I}_N \\ \mathbf{0}_N & \mathbf{I}_N \end{bmatrix} \overline{\mathbf{S}}_c \tag{38}$$

$$= \mathbf{Q}_c \left[\boldsymbol{\Omega}_c \ \ \boldsymbol{\Omega}_c\right] \overline{\mathbf{S}}_c. \tag{39}$$

The N independent jamming streams are precoded into the transmitted jamming signals according to the singular value decomposition of $\mathbf{H}_c$. More specifically, let us choose $\mathbf{X}_c$ as

$$\mathbf{X}_c = \overline{\mathbf{S}}_c^{-1} \begin{bmatrix} \mathbf{V}_c \\ -\mathbf{V}_c \end{bmatrix}, \tag{40}$$

where $\mathbf{V}_c$ is defined as in the previous section. Note that $\mathbf{X}_c \neq \mathbf{0}$ since $\overline{\mathbf{S}}_c^{-1}$ has $2N$ linearly independent (hence distinct) columns.

Substituting (39) and (40) in (1), the received signal vector at the legitimate receiver can be rewritten as

$$\mathbf{Y}_r = \mathbf{H}_t\mathbf{X}_t + \mathbf{Q}_c \left[\boldsymbol{\Omega}_c \ \ \boldsymbol{\Omega}_c\right] \begin{bmatrix} \mathbf{V}_c \\ -\mathbf{V}_c \end{bmatrix} + \mathbf{Z}_r \tag{41}$$

$$= \mathbf{H}_t\mathbf{X}_t + \mathbf{Z}_r. \tag{42}$$

The transmitted signal vector at the transmitter is given by (3). Using (2), (3), and (40), the received signal vector at the external eavesdropper is given by

$$\mathbf{Y}_e = \mathbf{G}_t\mathbf{P}_t\mathbf{U}_t + \mathbf{G}_c\overline{\mathbf{S}}_c^{-1}\bar{\mathbf{I}}\mathbf{V}_c + \mathbf{Z}_e, \tag{43}$$

where $\bar{\mathbf{I}} = \left[\mathbf{I}_N \quad -\mathbf{I}_N\right]^T$.

Note that $\overline{\mathbf{S}}_c^{-1}$ is a full rank matrix, hence, its $2N$ columns are linearly independent. The ith column of $\overline{\mathbf{S}}_c^{-1}\bar{\mathbf{I}}$ results from subtracting the $(i+N)$th column of $\overline{\mathbf{S}}_c^{-1}$ from its ith column, for all $i = 1, 2, \cdots, N$. Thus, the N columns of $\overline{\mathbf{S}}_c^{-1}\bar{\mathbf{I}}$ are linearly independent. Since all of the entries of $\mathbf{G}_c$ are drawn from a continuous distribution, $\mathbf{G}_c\overline{\mathbf{S}}_c^{-1}\bar{\mathbf{I}}$ is almost surely a full rank matrix, see the Appendix.

From (43), choosing the precoder $\mathbf{P}_t$ such that

$$\mathbf{P}_t = \mathbf{G}_t^{-1}\mathbf{G}_c\overline{\mathbf{S}}_c^{-1}\bar{\mathbf{I}} \tag{44}$$

perfectly aligns the information streams over the jamming ones at the eavesdropper. As previously mentioned, decoding the information streams at the legitimate receiver requires that $\mathbf{P}_t$ is a full rank matrix. Since both $\mathbf{G}_t^{-1}$ and $\mathbf{G}_c\overline{\mathbf{S}}_c^{-1}\bar{\mathbf{I}}$ are full rank, so is $\mathbf{P}_t$.

We observe that this approach simply amounts to choosing $\mathbf{J}_c = \overline{\mathbf{S}}_c^{-1}\bar{\mathbf{I}}$ in Section III. Hence, the analysis therein carries through resulting in the s.d.o.f. of N.

V. Removing One Antenna from The Cooperative Jammer

In the previous sections, we have been interested in identifying the number of antennas needed at the cooperative jammer to achieve the full d.o.f. of the channel in the presence of an eavesdropper. Here, we back away from the full d.o.f. and see that we can achieve close to full d.o.f. with fewer antennas at the cooperative jammer. Specifically, we provide an example scenario where we reduce the antennas at the cooperative jammer by one, i.e., $M = 2N - 1$, and show that $N - \frac{1}{2}$ d.o.f. is achievable.

The transmitted signal vector from the legitimate transmitter is given by (3), i.e., N independent information streams are sent from the transmitter. However, the null space of the channel matrix $\mathbf{H}_c$ has only $N-1$ dimensions. As mentioned previously, the jamming streams have to be transmitted over independent directions to guarantee a full rank precoding matrix at the transmitter. The cooperative jammer sets out to send $N-1$ jamming streams over the $N-1$ directions of the null space of $\mathbf{H}_c$ and send the remaining jamming stream over a direction that spatially aligns with one of the directions over which the information streams are received at the legitimate receiver. In addition, the direction over which this remaining jamming stream is sent has to be chosen such that the jamming and information streams occupy two rationally independent dimensions at the spatial direction over which they are aligned.

The signal transmitted by the cooperative jammer is given by

$$\mathbf{X}_c = \mathbf{J}_c\mathbf{V}_c^{(N-1)} + \mathbf{c}_N V_N, \tag{45}$$

where $\mathbf{J}_c \in \mathbb{R}^{(2N-1)\times(N-1)}$ is a matrix whose columns span $\mathcal{N}(\mathbf{H}_c)$. $\mathbf{V}_c^{(N-1)} = [V_1 \ \ V_2 \ \ \cdots \ \ V_{N-1}]^T$, where $V_1, V_2, \cdots, V_N$ are N i.i.d. jamming streams, each is uniformly distributed over the set $(-Q, Q)_{\mathbb{Z}}$. $\mathbf{c}_N \in \mathbb{R}^{2N-1}$ is a vector which does not belong $\mathcal{N}(\mathbf{H}_c)$ and will be chosen later in this section.

The received signal vector at the eavesdropper is

$$\mathbf{Y}_e = \mathbf{G}_t\mathbf{P}_t\mathbf{U}_t + \mathbf{G}_c\left[\mathbf{J}_c \quad \mathbf{c}_N\right] \begin{bmatrix} \mathbf{V}_c^{(N-1)} \\ V_N \end{bmatrix} + \mathbf{Z}_e. \tag{46}$$

Thus, the precoding matrix

$$\mathbf{P}_t = \mathbf{G}_t^{-1}\mathbf{G}_c\left[\mathbf{J}_c \quad \mathbf{c}_N\right] \tag{47}$$

aligns the information streams over the jamming signals at the eavesdropper. With similar arguments as in the previous sections, it can be shown that $\mathbf{P}_t$ is full rank.

The received signal at the legitimate receiver is given by

$$\mathbf{Y}_r = \mathbf{H}_t\mathbf{G}_t^{-1}\mathbf{G}_c\left[\mathbf{J}_c \quad \mathbf{c_N}\right] \begin{bmatrix} \mathbf{U}_t^{(N-1)} \\ U_N \end{bmatrix} + \mathbf{H}_c\mathbf{c}_N V_N + \mathbf{Z}_r, \tag{48}$$

where $\mathbf{U}_t^{(N-1)} = [U_1 \ U_2 \ \cdots \ U_{N-1}]^T$. The vector $\mathbf{c}_N$ is chosen from $\mathcal{N}(\mathbf{H}_t\mathbf{G}_t^{-1}\mathbf{G}_c - \gamma\mathbf{H}_c)$ such that

$$\mathbf{H}_t\mathbf{G}_t^{-1}\mathbf{G}_c\mathbf{c}_N = \gamma\mathbf{H}_c\mathbf{c}_N, \tag{49}$$

where γ is an arbitrary number that is rationally independent from 1. Thus, $\mathbf{c}_N$ does not belong to $\mathcal{N}(\mathbf{H}_c)$ almost surely.

The received signal signal vector at the legitimate receiver can be rewritten as

$$\mathbf{Y}_r = \left[\mathbf{H}_t\mathbf{G}_t^{-1}\mathbf{G}_c\mathbf{J}_c \quad \mathbf{H}_c\mathbf{c}_N\right] \begin{bmatrix} U_t^{(N-1)} \\ \gamma U_N + V_N \end{bmatrix} + \mathbf{Z}_r. \tag{50}$$

It can be shown that the mutual information between the transmitter and the legitimate receiver is given by

$$I(\mathbf{X}_t;\mathbf{Y}_r) \geq I(\mathbf{U}_t;\mathbf{Y}_r) \tag{51}$$

$$= I(\mathbf{U}_t^{(N-1)};\mathbf{Y}_r^{(N-1)}) + I(U_N;Y_{r_N}) + o(\log(P)), \tag{52}$$

where $\mathbf{Y}_r^{(N-1)} = [Y_{r_1}\ Y_{r_2}\ \cdots\ Y_{r_{N-1}}]^T$, Y_{r_i} is the received signal at the ith antenna of the legitimate receiver, $i = 1, 2, \cdots, N$. The first term on the right hand side of the above equation is equivalent to a point-to-point $(N-1)$-antenna AWGN channel, i.e., it provides $(N-1)$ d.o.f. The second term is equivalent to a single antenna AWGN channel with the information signal received over a rationally independent dimension from that of the interfering signal, and hence, provides $\frac{1}{2}$ d.o.f. [27]. From (46) and (47), the mutual information $I(\mathbf{X}_t, \mathbf{Y}_r)$ is upper bounded by N as in Section III. Thus, $N - \frac{1}{2}$ s.d.o.f. is achievable.

VI. Conclusion

In this paper, we have considered a Gaussian wiretap channel with N antennas at each of the transmitter, receiver and the external eavesdropper, and a cooperative jammer that has M antennas. We have considered achieving N secure degrees of freedom (s.d.o.f.) for this channel and identifying the number of antennas needed at the cooperative jammer, i.e., M, to achieve it. We have proposed the approach of sending the jamming signals over the null space of the channel matrix from the cooperative jammer to the legitimate receiver. We have shown that the secrecy penalty in the degrees of freedom of the channel can be completely compensated, i.e., an s.d.o.f. of N is achievable if $M = 2N$. The enablers for this achievability result have been choosing precoders for the transmitted and jamming signals carefully and the use of coordinated jamming signals in order to completely cover the transmitted signals at the eavesdropper while not interfering with the legitimate receiver. We have also shown that $N - \frac{1}{2}$ s.d.o.f. is achievable when the number of antennas at the cooperative jammer is reduced to $2N - 1$, achievable with discrete constellations and the use of real interference alignment in addition to spatial alignment. This last example demonstrates that a joint design of spatial and signal constellation alignment can be beneficial for secrecy for multiantenna Gaussian channels which is of current interest.

Appendix

Consider two matrices $\mathbf{A} \in \mathbb{R}^{N\times 2N}$ and $\mathbf{B} \in \mathbb{R}^{2N\times N}$ such that $\mathbf{A}$ is full row-rank and $\mathbf{B}$ has all of its entries independently drawn from a continuous distribution. We will show that $\mathbf{AB}$ is almost surely full rank. We have

$$\mathbf{A} = [\mathbf{a}_1\ \mathbf{a}_2\ \cdots\ \mathbf{a}_{2N}] \tag{53}$$

$$\mathbf{B} = [\mathbf{b}_1\ \mathbf{b}_2\ \cdots\ \mathbf{b}_N], \tag{54}$$

where $\mathbf{a}_1, \mathbf{a}_2, \cdots, \mathbf{a}_{2N}$ are the $2N$ length-N columns of $\mathbf{A}$ while $\mathbf{b}_1, \mathbf{b}_2, \cdots, \mathbf{b}_N$ are the N length-$2N$ columns of $\mathbf{B}$.

Let $b_{j,i}$ denote the entry in the jth row and ith column of $\mathbf{B}$. Let $\mathbf{AB} = [\mathbf{c}_1\ \mathbf{c}_2\ \cdots \mathbf{c}_N]$, where $\mathbf{c}_i$ is a length-N column vector, for $i = 1, 2, \cdots, N$. In order to show that the matrix $\mathbf{AB}$ is almost surely full rank, we need to show that the N columns $\{\mathbf{c}_i, i = 1, \cdots, N\}$ are linearly independent, i.e.,

$$\sum_{i=1}^{N} \alpha_i \mathbf{c}_i = 0 \tag{55}$$

if and only if $\alpha_i = 0$ for all $i = 1, 2, \cdots, N$.

Each $\mathbf{c}_i$, for $i = 1, 2, \cdots, N$, can be viewed as a linear combination of the $2N$ columns of $\mathbf{A}$ with coefficients that are the entries of the column $\mathbf{b}_i$ of $\mathbf{B}$, i.e.,

$$\mathbf{c}_i = \sum_{j=1}^{2N} b_{j,i}\mathbf{a}_j. \tag{56}$$

Using (56), we can rewrite (55) as

$$\sum_{j=1}^{2N} m_j \mathbf{a}_j = 0 \tag{57}$$

where, for all $j = 1, 2, \cdots, 2N$,

$$m_j = \sum_{i=1}^{N} \alpha_i b_{j,i}. \tag{58}$$

The $2N$ columns of $\mathbf{A}$ are linearly dependent since each of them of length N. Therefore, the equation (57) has infinitely many solutions for $\{m_j\}_{j=1}^{2N}$.

Each of these solutions for m_j's constitutes a system of $2N$ linear equations $\{m_j = \sum_{i=1}^{N} \alpha_i b_{j,i},\ j = 1, 2, \cdots, 2N\}$. The number of unknowns in this system, i.e. α's, is N. Since the number of equations of this system is greater than the number of unknowns, this system has a solution for $\{\alpha_i\}_{i=1}^{N}$ if and only if the elements $b_{j,i}, j = 1, 2, \cdots, 2N, i = 1, 2, \cdots, N$ have some structure, i.e., are dependent. Since the entries of $\mathbf{B}$ are all independently drawn from some continuous distribution, the probability that these entries being dependent is zero.

Moreover, consider the set with infinite cardinality, where each element in this set is a structured set $\mathbf{B}$ that causes the system of equations in (58) to have a solution for $\{\alpha_i\}$, for one of the infinitely many solutions of $\{m_j\}$ to (57). This set with infinite cardinality has a Lebesgue measure zero in the space $\mathbb{R}^{2N\times N}$ since this set is a subspace of $\mathbb{R}^{2N\times N}$ with a dimension strictly less than $2N \times N$. We conclude that (55) almost surely has no non-zero solution for $\{\alpha_i\}$. Thus, $\mathbf{AB}$ is almost surely a full rank matrix.

If $\mathbf{AB}$ is almost surely full rank, then $(\mathbf{AB})^T = \mathbf{B}^T\mathbf{A}^T$ is also almost surely full rank. Hence, if two matrices $\mathbf{C} \in \mathbb{R}^{N\times 2N}$and $\mathbf{D} \in \mathbb{R}^{2N\times N}$ are such that $\mathbf{C}$ has all of its entries independently drawn from a continuous distribution and $\mathbf{D}$ is full column-rank, then $\mathbf{CD}$ is almost surely full rank.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[3] I. Csiszar and J. Korner, “Broadcast channels with confidential messages,” *IEEE Trans. Info. Theory*, vol. 24, no. 3, pp. 339–3487, 1978.

[4] S. Leung-Yan-Cheong and M. Hellman, “The Gaussian wire-tap channel,” *IEEE Trans. Info. Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[5] E. Tekin, S. Serbetli, and A. Yener, “On secure signaling for the Gaussian multiple access wire-tap channel,” in *2005 Asilomar Conf. on Signals, Systems, and Computers*, Nov. 2005, pp. 1747–1751.

[6] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, “Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions,” *IEEE Trans. Info. Theory*, vol. 54, no. 6, pp. 2493–2507, 2008.

[7] O. O. Koyluoglu and H. El Gamal, “Cooperative encoding for secrecy in interference channels,” *IEEE Trans. Info. Theory*, vol. 57, no. 9, pp. 5682–5694, 2011.

[8] X. He and A. Yener, “A new outer bound for the Gaussian interference channel with confidential messages,” in *43rd Annual Conference on Information Sciences and Systems. CISS*, Mar. 2009, pp. 318–323.

[9] E. Tekin and A. Yener, “Achievable rates for the general Gaussian multiple access wire-tap channel with collective secrecy,” in *44th Annual Allerton Conf. On Communication, Control, and Computing*, Sep. 2006, pp. 809–816.

[10] ——, “The Gaussian multiple access wire-tap channel,” *IEEE Trans. Info. Theory*, vol. 54, no. 12, pp. 5747–5755, 2008.

[11] ——, “The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming,” *IEEE Trans. Info. Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

[12] E. Ekrem and S. Ulukus, “Secrecy in cooperative relay broadcast channels,” *IEEE Trans. Info. Theory*, vol. 57, no. 1, pp. 137–155, 2011.

[13] X. He and A. Yener, “End-to-end secure multi-hop communication with untrusted relays,” *IEEE Trans. Wireless Communications*, vol. 12, no. 1, pp. 1–11, 2013.

[14] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, “Interference alignment for secrecy,” *IEEE Trans. Info. Theory*, vol. 57, no. 6, pp. 3323–3332, 2011.

[15] X. He and A. Yener, “Secure degrees of freedom for Gaussian channels with interference: Structured codes outperform Gaussian signaling,” in *IEEE Global Telecommunications Conference. GLOBECOM*, Dec. 2009, pp. 1–6.

[16] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, “On the secure degrees-of-freedom of the multiple-access-channel,” *Submitted to IEEE Trans. Info. Theory*, 2010, arXiv preprint arXiv:1003.0729.

[17] J. Xie and S. Ulukus, “Secure degrees of freedom of one-hop wireless networks,” *Submitted to IEEE Trans. Info. Theory*, 2012, arXiv preprint arXiv:1209.5370.

[18] ——, “Secure degrees of freedom of K-user Gaussian interference channels: A unified view,” *Submitted to IEEE Trans. Info. Theory*, 2013, arXiv preprint arXiv:1305.7214.

[19] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, “The Gaussian wiretap channel with a helping interferer,” in *IEEE International Symposium on Information Theory. ISIT*, Jul. 2008, pp. 389–393.

[20] X. He and A. Yener, “Providing secrecy with structured codes: Tools and applications to two-user Gaussian channels,” *Submitted to IEEE Trans. Info. Theory*, 2009, arXiv preprint arXiv:0907.5388.

[21] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” *IEEE Trans. Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, 2008.

[22] M. Nafea and A. Yener, “Degrees of freedom of the single antenna Gaussian wiretap channel with a helper irrespective of the number of antennas at the eavesdropper,” *to appear in IEEE GlobalSIP Symposium on Cyber-Security and Privacy*, Dec. 2011.

[23] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas-Part II: The MIMOME wiretap channel,” *IEEE Trans. Info. Theory*, vol. 56, no. 11, pp. 5515–5532, 2010.

[24] F. Oggier and B. Hassibi, “The secrecy capacity of the MIMO wiretap channel,” *IEEE Trans. Info. Theory*, vol. 57, no. 8, pp. 4961–4972, 2011.

[25] T. Liu and S. Shamai, “A note on the secrecy capacity of the multiple-antenna wiretap channel,” *IEEE Trans. Info. Theory*, vol. 55, no. 6, pp. 2547–2553, 2009.

[26] S. Shafiee, N. Liu, and S. Ulukus, “Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel,” *IEEE Trans. Info. Theory*, vol. 55, no. 9, pp. 4033–4039, 2009.

[27] A. S. Motahari, S. O. Gharan, and A. K. Khandani, “Real interference alignment with real numbers,” *Submitted to IEEE Trans. Info. Theory*, 2009, arXiv preprint arXiv:0908.1208.